

# Extending Clause Learning SAT Solvers with Complete Parity Reasoning (extended version)

Tero Laitinen, Tommi Junttila, and Ilkka Niemelä

Aalto University

Department of Information and Computer Science

PO Box 15400, FI-00076 Aalto, Finland

Email: {Tero.Laitinen,Tommi.Junttila,Ilkka.Niemela}@aalto.fi

**Abstract**—Instances of logical cryptanalysis, circuit verification, and bounded model checking can often be succinctly represented as a combined satisfiability (SAT) problem where an instance is a combination of traditional clauses and parity constraints. This paper studies how such combined problems can be efficiently solved by augmenting a modern SAT solver with an xor-reasoning module in the DPLL(XOR) framework. A new xor-reasoning module that deduces all possible implied literals using incremental Gauss-Jordan elimination is presented. A decomposition technique that can greatly reduce the size of parity constraint matrices while allowing still to deduce all implied literals is presented. It is shown how to eliminate variables occurring only in parity constraints while preserving the decomposition. The proposed techniques are evaluated experimentally.

## I. INTRODUCTION

Propositional satisfiability (SAT) solvers (see e.g. [1]) provide a powerful solution technique in many industrial application domains. Representing an instance of propositional satisfiability in conjunctive normal form (CNF) allows very efficient Boolean constraint propagation and conflict-driven clause learning (CDCL) techniques. However, CNF-based solvers can scale poorly on instances consisting on straightforward CNF-encoding of parity (xor) constraints [2]. Such xor-constraints occur frequently in domains such as logical cryptanalysis, circuit verification, and bounded model checking. Considering this and recalling that an instance consisting only of xor-constraints can be solved in polynomial time using Gaussian elimination, it is no wonder that many approaches for combining CNF-level and xor-constraint reasoning have been presented [3], [4], [5], [6], [7], [8], [9], [10], [11], [12], [13], [14]. These approaches extend CNF-level SAT solvers by implementing different forms of constraint propagation for xor-constraints, ranging from plain unit propagation via equivalence reasoning to Gaussian elimination. Compared to unit propagation, which has efficient implementation techniques, equivalence reasoning and Gaussian elimination allow stronger propagation but are computationally much more costly.

In this paper we make two contributions in this field. First, we present an xor-reasoning technique based on Gauss-Jordan elimination that provides complete constraint propagation for xor-constraints in the following sense: Given a conjunction  $\phi_{\text{xor}}$  of xor-constraints and values for some of its variables (so-called xor-assumptions provided by the CNF-level master search engine), the module can (i) *decide* whether  $\phi_{\text{xor}}$  is sat-

isfiable under the xor-assumptions, and (ii) find *all* the literals and equivalences implied by  $\phi_{\text{xor}}$  and the xor-assumptions. This is better than (i) equivalence reasoning which cannot always decide the satisfiability or find all the implied literals, and (ii) Gaussian elimination which can decide satisfiability but not necessarily finds all the implied literals (as illustrated in Sect. III).<sup>1</sup>

Our second contribution is a new decomposition theorem that sometimes allows us to split the xor-constraint part  $\phi_{\text{xor}}$  into components that can be handled individually. This technique supersedes the well-known “connected components” approach that exploits variable disjoint components of  $\phi_{\text{xor}}$ . Instead, we use a variant of “biconnected components” by splitting  $\phi_{\text{xor}}$  into components that can be connected to each other only by single cut variables. We prove that if we can provide full propagation for each of the components, we have full propagation for the whole xor-part  $\phi_{\text{xor}}$  as well. We show how the structure of biconnected components can be preserved while eliminating most of the variables occurring only in the xor-part leading to more compact representation of the formula. The presented xor-reasoning, decomposition, and variable elimination techniques are evaluated experimentally on large sets of benchmark instances. The proofs of Lemmas and Theorems can be found in the appendix.

## II. PRELIMINARIES

Let  $\mathbb{B} = \{\perp, \top\}$  be the set of truth values “false” and “true”. A literal is a Boolean variable  $x$  or its negation  $\neg x$  (as usual,  $\neg\neg x$  will mean  $x$ ), and a clause is a disjunction of literals. If  $\phi$  is any kind of formula or equation, (i)  $\text{vars}(\phi)$  is the set of variables occurring in it, (ii)  $\text{lits}(\phi) = \{x, \neg x \mid x \in \text{vars}(\phi)\}$  is the set of literals over  $\text{vars}(\phi)$ , and (iii) a truth assignment for  $\phi$  is a, possibly partial, function  $\tau : \text{vars}(\phi) \rightarrow \mathbb{B}$ . A truth assignment satisfies (i) a variable  $x$  if  $\tau(x) = \top$ , (ii) a literal  $\neg x$  if  $\tau(x) = \perp$ , and (iii) a clause  $(l_1 \vee \dots \vee l_k)$  if it satisfies at least one literal  $l_i$  in the clause.

An *xor-constraint* is an equation of form  $x_1 \oplus \dots \oplus x_k \equiv p$ , where the  $x_i$ s are Boolean variables and  $p \in \mathbb{B}$  is the parity.<sup>2</sup>

<sup>1</sup>We’ve just learned that the use of Gauss-Jordan has also been independently discovered in [15]: the main difference to our work is that we (i) do not consider Craig interpolants but (ii) can also find all the implied equivalences.

<sup>2</sup>The correspondence of xor-constraints to the “xor-clause” representation used e.g. in [11], [13], [14] is straightforward:  $x_1 \oplus \dots \oplus x_k \equiv \top$  corresponds to the xor-clause  $(x_1 \oplus \dots \oplus x_k)$  and  $x_1 \oplus \dots \oplus x_k \equiv \perp$  to  $(x_1 \oplus \dots \oplus x_k \oplus \top)$ .

We implicitly assume that duplicate variables are always removed from the equations, e.g.  $x_1 \oplus x_2 \oplus x_1 \oplus x_3 \equiv \top$  is always simplified into  $x_2 \oplus x_3 \equiv \top$ . If the left hand side does not have variables, then it equals to  $\perp$ ; the equation  $\perp \equiv \top$  is a contradiction and  $\perp \equiv \perp$  a tautology. We identify the xor-constraint  $x \equiv \top$  with the literal  $x$  and  $x \equiv \perp$  with  $\neg x$ . A truth assignment  $\tau$  satisfies an xor-constraint ( $x_1 \oplus \dots \oplus x_k \equiv p$ ) if  $\tau(x_1) \oplus \dots \oplus \tau(x_k) = p$ .

A *cnf-xor formula* is a conjunction  $\phi_{\text{or}} \wedge \phi_{\text{xor}}$ , where  $\phi_{\text{or}}$  is a conjunction of clauses and  $\phi_{\text{xor}}$  is a conjunction of xor-constraints. A truth assignment satisfies  $\phi_{\text{or}} \wedge \phi_{\text{xor}}$  if it satisfies every clause and xor-constraint in it.

### A. DPLL(XOR) and Xor-Reasoning Modules

We are interested in solving the satisfiability of cnf-xor formulas of the form  $\phi_{\text{or}} \wedge \phi_{\text{xor}}$  defined above. Similarly to the DPLL( $T$ ) approach for Satisfiability Modulo Theories, see e.g. [16], [17], the DPLL(XOR) approach [11] for solving cnf-xor formulas consists of (i) a conflict-driven clause learning (CDCL) SAT solver that takes care of solving the CNF-part  $\phi_{\text{or}}$ , and (ii) an *xor-reasoning module* that handles the xor-part  $\phi_{\text{xor}}$ . The CDCL solver is the master process, responsible of guessing values for the variables according to some heuristics (“branching”), performing propagation in the CNF-part, conflict analysis, restarts etc. The xor-reasoning module receives variable values, called xor-assumptions, from the CDCL solver and checks (i) whether the xor-part can still be satisfied under the xor-assumptions, and (ii) whether some variable values, called xor-implied literals, are implied by the xor-part and the xor-assumptions. These checks can be incomplete, like in [11], [13] for the satisfiability and in [11], [13], [10] for the implication checks, as long as the satisfiability check is complete when all the variables have values.

The very basic interface for an xor-reasoning module can consist of the following methods:

- `init( $\phi_{\text{xor}}$ )` initializes the module with  $\phi_{\text{xor}}$ . It may return “unsat” if it finds  $\phi_{\text{xor}}$  unsatisfiable, or a set of *xor-implied literals*, i.e. literals  $\hat{l}$  such that  $\phi_{\text{xor}} \models \hat{l}$  holds.
- `assume( $\tilde{l}$ )` is used to communicate a new variable value  $\tilde{l}$  deduced in the CNF solver part to the xor-reasoning module. This value, called *xor-assumption* literal  $\tilde{l}$ , is added to the list of current xor-assumptions. If  $[\tilde{l}_1, \dots, \tilde{l}_k]$  are the current xor-assumptions, the module then tries to (i) deduce whether  $\phi_{\text{xor}} \wedge \tilde{l}_1 \wedge \dots \wedge \tilde{l}_k$  became unsatisfiable, i.e. whether an *xor-conflict* was encountered, and if this was not the case, (ii) find *xor-implied literals*, i.e. literals  $\hat{l}$  for which  $\phi_{\text{xor}} \wedge \tilde{l}_1 \wedge \dots \wedge \tilde{l}_k \models \hat{l}$  holds. The xor-conflict or the xor-implied literals are then returned to the CNF solver part so that it can start conflict analysis (in the case of xor-conflict) or extend its current partial truth assignment with the xor-implied literals.

In order to facilitate conflict-driven backjumping and clause learning in the CNF solver part, the xor-reasoning module has to provide a clausal *explanation* for each xor-conflict and xor-implied literal it reports. That is,

- if  $\phi_{\text{xor}} \wedge \tilde{l}_1 \wedge \dots \wedge \tilde{l}_k$  is deduced to be unsatisfiable, then the module must report a (possibly empty) clause  $(\neg l'_1 \vee \dots \vee \neg l'_m)$  such that (i) each  $l'_i$  is an xor-assumption or an xor-implied literal, and (ii)  $\phi_{\text{xor}} \wedge \tilde{l}_1 \wedge \dots \wedge \tilde{l}_k \models (\neg l'_1 \vee \dots \vee \neg l'_m)$ ; and
- if it was deduced that  $\phi_{\text{xor}} \wedge \tilde{l}_1 \wedge \dots \wedge \tilde{l}_k \models \hat{l}$  for some  $\hat{l}$ , then the module must report a clause  $(\neg l'_1 \vee \dots \vee \neg l'_m \vee \hat{l})$  such that (i) each  $l'_i$  is an xor-assumption or an xor-implied literal reported earlier, and (ii)  $\phi_{\text{xor}} \wedge \tilde{l}_1 \wedge \dots \wedge \tilde{l}_k \models \hat{l}$ , i.e.  $\phi_{\text{xor}} \models (\neg l'_1 \vee \dots \vee \neg l'_m \vee \hat{l})$ .
- `backtrack()` retracts the latest xor-assumption and all the xor-implied literals deduced after it.

Naturally, variants of this interface are easily conceivable. For instance, a larger set of xor-assumptions can be given with the `assume` method at once instead of only one.

For xor-reasoning modules based on equivalence reasoning, see [11], [13]. The Gaussian elimination process in [10], [12] can also be easily seen as an xor-reasoning module.

### III. INCREMENTAL GAUSS-JORDAN ELIMINATION

We now develop an xor-reasoning technique that can, given a conjunction  $\phi_{\text{xor}}$  of xor-constraints and a conjunction  $\tilde{l}_1 \wedge \dots \wedge \tilde{l}_k$  of xor-assumption literals, (i) *decide* whether  $\phi_{\text{xor}} \wedge \tilde{l}_1 \wedge \dots \wedge \tilde{l}_k$  is satisfiable or not, and (ii) if it is, to find *all* the literals and equivalences implied by  $\phi_{\text{xor}} \wedge \tilde{l}_1 \wedge \dots \wedge \tilde{l}_k$ . The proposed technique can be seen as an incremental, Boolean-level version of the Gauss-Jordan elimination process, or a Boolean-level variant of the linear arithmetic solver described in [18].

Before going into the details, let us first briefly note why Gaussian elimination, used e.g. in Cryptominisat [10], [12] version 2.9.2, is not enough to find all the implied literals (although it can detect unsatisfiability perfectly). Basically, the reason is that Gaussian elimination presents the xor-constraints in  $\phi_{\text{xor}}$  with a row echelon form matrix, where pivoting upwards is not performed. As an example, consider the row echelon form matrix-like representation

$$\begin{array}{rcl} x_1 \oplus x_2 & \oplus x_4 & \equiv \top \\ x_2 \oplus x_3 & \oplus x_5 & \equiv \perp \\ x_3 \oplus x_4 \oplus x_5 & & \equiv \top \end{array}$$

for a conjunction  $\phi_{\text{xor}}$  of xor-constraints. It is easy to deduce from this that  $\phi_{\text{xor}}$  is satisfiable but not that  $x_1$  must always be false, i.e. that  $\phi_{\text{xor}} \models x_1 \equiv \perp$ .

#### A. Tableaux i.e. Reduced Row Echelon Form Matrices

We begin by giving an equation form representation and the basic operations we need for reduced row echelon matrices. A *tableau* for a satisfiable conjunction  $\phi_{\text{xor}}$  of xor-constraints is a set  $\mathcal{E}$  of equations of form  $x_i := x_{i,1} \oplus \dots \oplus x_{i,k_i} \oplus p_i$ , where  $x_i, x_{i,1}, \dots, x_{i,k_i}$  are distinct variables in  $\phi_{\text{xor}}$  and  $p_i \in \mathbb{B}$ . Furthermore, it is required that

- 1) each variable  $x \in \text{vars}(\phi_{\text{xor}})$  occurs *at most once* as the left hand side variable in the equations in  $\mathcal{E}$ ,

- 2) if a variable  $x \in \text{vars}(\phi_{\text{xor}})$  occurs as the left hand side variable in an equation, then it does not occur in the right hand side of any equation, and
- 3)  $\bigwedge_{x_i := x_{i,1} \oplus \dots \oplus x_{i,k_i} \oplus p_i \in \mathcal{E}} (x_i \oplus x_{i,1} \oplus \dots \oplus x_{i,k_i} \equiv p_i)$  is logically equivalent to  $\phi_{\text{xor}}$ .

The variables of  $\phi_{\text{xor}}$  occurring as left hand side variables in the equations are called *basic variables* while the others are *non-basic variables* in  $\mathcal{E}$ . If  $\mathcal{E}$  has  $n$  non-basic variables, then  $\phi_{\text{xor}}$  has  $2^n$  satisfying truth assignments. Observe that a tableau can be seen as a linear arithmetic modulo 2 matrix equation; under a variable order where basic variables are first, the matrix will be in the reduced row echelon form.

*Example 1:* Take the conjunction  $(a \oplus c \oplus e \equiv \top) \wedge (a \oplus b \oplus d \oplus e \equiv \top)$ . A tableau for it is  $\left\{ \begin{array}{l} a := c \oplus e \oplus \top \\ b := c \oplus d \oplus \perp \end{array} \right\}$ , or  $\begin{pmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 \end{pmatrix} \begin{pmatrix} a & b & c & d & e \end{pmatrix}^T = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$  as a matrix equation; the first matrix is in the reduced row echelon form.

Given a conjunction  $\phi_{\text{xor}} = D_1 \wedge \dots \wedge D_m$  of xor-constraints, it is easy to build a tableau for it (or to detect that the conjunction is unsatisfiable, in which case it does not have a tableau). We start with the empty tableau, and for each xor-constraint  $D$  in the conjunction apply the following:

- 1) Eliminate each basic variable  $x_i$  in  $D$  by substituting it with the right hand side of the equation  $x_i := x_{i,1} \oplus \dots \oplus x_{i,k_i} \oplus p_i$  already in the tableau, then simplify the resulting xor-constraint.
- 2) (i) If the resulting xor-constraint is  $(\perp \equiv \perp)$ , then  $D$  is a linear combination of the xor-constraints already in the tableau and nothing is added in the tableau.  
(ii) If the resulting xor-constraint is  $(\perp \equiv \top)$ , then  $D$  is contradicting the xor-constraints already in the tableau and the conjunction  $\phi_{\text{xor}}$  is unsatisfiable.  
(iii) Otherwise, all the variables in the resulting xor-constraint  $(y_1 \oplus y_2 \oplus \dots \oplus y_k \equiv p)$  are non-basic variables. Pick one of these variables, say  $y_1$ , insert the equation  $y_1 := y_2 \oplus \dots \oplus y_k \oplus p$  in the tableau, eliminate  $y_1$  from the right hand sides of other equations by substituting it with  $y_2 \oplus \dots \oplus y_k \oplus p$ , and simplify the right hand sides of the equations.

*Example 2:* Take again the satisfiable conjunction  $(a \oplus c \oplus e \equiv \top) \wedge (a \oplus b \oplus d \oplus e \equiv \top)$ . When inserting  $(a \oplus c \oplus e \equiv \top)$  into the empty tableau, we may select  $a$  to be the basic variable and get the tableau  $\{a := c \oplus e \oplus \top\}$ . Next inserting  $(a \oplus b \oplus d \oplus e \equiv \top)$ , we first substitute  $a$  with its definition  $c \oplus e \oplus \top$ , get  $(b \oplus c \oplus d \equiv \perp)$ , select  $b$  to be a basic variable, and obtain the tableau  $\{a := c \oplus e \oplus \top, b := c \oplus d \oplus \perp\}$ .

In the following, we must be able to transform a basic variable into a non-basic one. To do this, we must make a non-basic variable basic. If  $x$  is a basic variable with the equation  $x := y_1 \oplus \dots \oplus y_i \oplus \dots \oplus y_k \oplus p$  in a tableau  $\mathcal{E}$ , we define  $\text{swap}(\mathcal{E}, x, y_i)$  to be the tableau obtained as follows:

- 1) remove  $x := y_1 \oplus \dots \oplus y_i \oplus \dots \oplus y_k \oplus p$  from  $\mathcal{E}$ ,
- 2) add  $y_i := y_1 \oplus \dots \oplus y_{i-1} \oplus x \oplus y_{i+1} \oplus \dots \oplus y_k \oplus p$  in  $\mathcal{E}$ , and
- 3) remove  $y_i$  from the right hand sides of the other equa-

tions by substituting its occurrences with  $y_1 \oplus \dots \oplus y_{i-1} \oplus x \oplus y_{i+1} \oplus \dots \oplus y_k \oplus p$ .

*Example 3:* If  $\mathcal{E} = \left\{ \begin{array}{l} a := c \oplus e \oplus \top \\ b := c \oplus d \oplus \perp \end{array} \right\}$ , then we have  $\text{swap}(\mathcal{E}, b, c) = \left\{ \begin{array}{l} a := b \oplus d \oplus e \oplus \top \\ c := b \oplus d \oplus \perp \end{array} \right\}$ .

## B. Handling Xor-Assumptions: Assigned Tableaux

We now show how to handle xor-assumptions, i.e. to *decide* whether  $\phi_{\text{xor}} \wedge \tilde{l}_1 \wedge \dots \wedge \tilde{l}_k$  is still satisfiable, and if yes, to find *all* the literals and equivalences implied by  $\phi_{\text{xor}} \wedge \tilde{l}_1 \wedge \dots \wedge \tilde{l}_k$ . To do these, we introduce a concept of assigned tableaux. To facilitate easy backtracking, i.e. removal of xor-assumptions, the key idea here, similarly to [18], is to not remove variables from the tableau when new xor-assumptions are made but handle them separately. In this way backtracking simply amounts to retracting xor-assumptions.

Formally, an *assigned tableau* for  $\phi_{\text{xor}}$  is a pair  $\langle \mathcal{E}, \tau \rangle$  such that (i)  $\mathcal{E}$  is a tableau for  $\phi_{\text{xor}}$ , and (ii)  $\tau$  is a, usually partial, truth assignment for  $\phi_{\text{xor}}$  in which we collect the xor-assumptions and xor-implied literals. With respect to  $\langle \mathcal{E}, \tau \rangle$ , an equation  $x_i := x_{i,1} \oplus \dots \oplus x_{i,k_i} \oplus p_i \in \mathcal{E}$  is *propagation saturated* if it holds that  $\tau(x_i)$  is defined if and only if  $\tau(x_{i,j})$  is defined for all  $x_{i,j} \in \{x_i, x_{i,1}, \dots, x_{i,k_i}\}$ ; the assigned tableau  $\langle \mathcal{E}, \tau \rangle$  is *propagation saturated* if each equation in it is. An equation  $x_i := x_{i,1} \oplus \dots \oplus x_{i,k_i} \oplus p_i$  is *inconsistent* if  $\tau(x)$  is defined for all  $x \in \{x_i, x_{i,1}, \dots, x_{i,k_i}\}$  and  $\tau(x_i) \neq \tau(x_{i,1}) \oplus \dots \oplus \tau(x_{i,k_i}) \oplus p_i$ ; if the equation is not inconsistent, it is *consistent*. An assigned tableau is inconsistent if it has an inconsistent equation; otherwise it is consistent. A key property of a propagation saturated assigned tableau  $\langle \mathcal{E}, \tau \rangle$  is that its consistency is in one-to-one correspondence with the satisfiability of  $\phi_{\text{xor}}$  under the truth assignment  $\tau$ :

*Lemma 1:* Let  $\langle \mathcal{E}, \tau \rangle$  be a propagation saturated assigned tableau for  $\phi_{\text{xor}}$ . The formula  $\phi_{\text{xor}} \wedge \bigwedge_{(x \mapsto v_x) \in \tau} (x \equiv v_x)$  is satisfiable if and only if  $\langle \mathcal{E}, \tau \rangle$  is consistent.

From a consistent, propagation saturated assigned tableau it is also easy to enumerate *all* the literals that are implied by the xor-constraints and the truth assignment in the tableau:

*Lemma 2:* Let  $\langle \mathcal{E}, \tau \rangle$  be a consistent, propagation saturated assigned tableau for  $\phi_{\text{xor}}$ . For each literal  $y \equiv v_y$  it holds that  $\phi_{\text{xor}} \wedge \bigwedge_{(x \mapsto v_x) \in \tau} (x \equiv v_x) \models (y \equiv v_y)$  if and only if  $\tau(y) = v_y$ .

In addition to implied literals, we can also enumerate all implied binary xor-constraints (i.e., equalities and disequalities between variables) as the following Lemma shows.

*Lemma 3:* Let  $\langle \mathcal{E}, \tau \rangle$  be a consistent, propagation saturated assigned tableau for  $\phi_{\text{xor}}$ . For any two distinct variables  $y, z$  and any  $p \in \mathbb{B}$ , it holds that  $\phi_{\text{xor}} \wedge \bigwedge_{(x \mapsto v_x) \in \tau} (x \equiv v_x) \models (y \oplus z \equiv p)$  if and only if

- 1)  $\tau(y)$  and  $\tau(z)$  are both defined and  $\tau(y) \oplus \tau(z) = p$ ,
- 2)  $\tau(y)$  and  $\tau(z)$  are undefined and  $\mathcal{E}$  has an equation  $e$  of form  $y := \dots \oplus z \oplus \dots$  such that  $e|_\tau$  is  $y := z \oplus p$ , where  $e|_\tau$  is the equation obtained from  $e$  by substituting the variables in it assigned by  $\tau$  with their values,

- 3)  $\tau(y)$  and  $\tau(z)$  are undefined and  $\mathcal{E}$  has an equation  $e$  of form  $z := \dots \oplus y \oplus \dots$  such that  $e|_\tau$  is  $z := y \oplus p$ , or
- 4)  $\tau(y)$  and  $\tau(z)$  are undefined and  $\mathcal{E}$  has two equations,  $e_y$  and  $e_z$ , of forms  $y := \dots$  and  $z := \dots$  such that  $e_y|_\tau$  is  $y := f$ ,  $e_z|_\tau$  is  $z := g$ , and  $f \oplus g$  equals  $p$ .

*Example 4:* Consider the assigned tableau  $\langle \mathcal{E}, \tau \rangle$  for a  $\phi_{\text{xor}}$  with  $\mathcal{E} = \{x_1 := x_3 \oplus x_4 \oplus \top, x_2 := x_3 \oplus x_4 \oplus x_5 \oplus \top\}$  and  $\tau = \{x_5 \mapsto \top\}$ . Now  $\phi_{\text{xor}} \wedge (x_5 \equiv \top) \models (x_1 \oplus x_2 \equiv \top)$  as  $(x_1 := x_3 \oplus x_4 \oplus \top)|_\tau$  is  $x_1 := x_3 \oplus x_4 \oplus \top$ ,  $(x_2 := x_3 \oplus x_4 \oplus x_5 \oplus \top)|_\tau$  is  $x_2 := x_3 \oplus x_4 \oplus \top$ , and  $(x_3 \oplus x_4 \oplus \top) \oplus (x_3 \oplus x_4 \oplus \top)$  equals  $\top$ .

Such implied binary xor-constraints can be used to preprocess the cnf-xor formula and possibly also during the search; this topic is left for future research.

1) *Making the initial assigned tableau:* If we have a tableau for  $\phi_{\text{xor}}$  (implying that  $\phi_{\text{xor}}$  is satisfiable), we get a corresponding consistent, propagation saturated assigned tableau  $\langle \mathcal{E}, \tau \rangle$  by simply setting  $\tau(x_i) = p_i$  for each equation  $x_i := p_i$  in  $\mathcal{E}$ .

*Example 5:* For  $\phi_{\text{xor}} = (x \oplus y \oplus z \equiv \top) \wedge (y \oplus z \equiv \perp)$  we may get the tableau  $\{x := \top, y := z \oplus \perp\}$ . The corresponding consistent, propagation saturated assigned tableau is thus  $\langle \{x := \top, y := z \oplus \perp\}, \{x \mapsto \top\} \rangle$ .

2) *Extending with new xor-assumptions:* We now describe the central operation of extending a consistent, propagation saturated assigned tableau with a new xor-assumption. Given such an assigned tableau  $\langle \mathcal{E}, \tau \rangle$  and an xor-assumption literal  $x \equiv v$ , define  $\text{extend}(\langle \mathcal{E}, \tau \rangle, x \equiv v)$  to be a result of the following non-deterministic method  $\text{assume}(x \equiv v)$ :

- 1) If  $\tau(x) = v$ , return “sat, no new xor-implied literals”.
- 2) If  $\tau(x) \neq v$ , return “unsat”.
- 3) If  $x$  is a basic variable in  $\mathcal{E}$ , update  $\mathcal{E}$  to  $\text{swap}(\mathcal{E}, x, y)$ , where  $y$  is any  $\tau$ -unassigned non-basic variable in the equation for  $x$ ;  $x$  is now a non-basic variable.
- 4) Assign  $\tau(x) = v$ .
- 5) For each equation  $z := x \oplus x'_1 \oplus \dots \oplus x'_m \oplus p$  in  $\mathcal{E}$ , check whether  $\tau(x'_i)$  is defined for each variable  $x'_i$  occurring in the right hand side; if this is the case, evaluate the value  $v_z$  of  $z$  according to the equation and assign  $\tau(z) = v_z$ . The literal  $z \equiv v_z$  is a new xor-implied literal.
- 6) Return “sat” and all the new xor-implied literals found.

*Example 6:* Consider the consistent, propagation saturated assigned tableau  $\langle \mathcal{E}_0, \emptyset \rangle$ , where  $\mathcal{E}_0 = \left\{ \begin{array}{ll} a := d & \oplus f \oplus \top \\ b := d \oplus e & \oplus \perp \\ c := d & \oplus f \oplus \perp \end{array} \right\}$ .

To compute  $\text{extend}(\langle \mathcal{E}_0, \emptyset \rangle, a \equiv \top)$ , we first make the variable  $a$  non-basic by transforming  $\mathcal{E}_0$  to  $\mathcal{E}_1 = \text{swap}(\mathcal{E}_0, a, d) = \left\{ \begin{array}{ll} d := a & \oplus f \oplus \top \\ b := a \oplus e \oplus f \oplus \top \\ c := a & \oplus \top \end{array} \right\}$  and then assign  $a$  to  $\top$ ; the resulting consistent, but not propagation saturated, assigned tableau is  $\langle \mathcal{E}_1, \{a \mapsto \top\} \rangle$ . To make it propagation saturated, we note that  $c := a \oplus \top$  has all its right hand side variables assigned and deduce a value for  $c$ , resulting in  $\langle \mathcal{E}_1, \{a \mapsto \top, c \mapsto \perp\} \rangle$ .

3) *Backtracking:* Now observe the following: once an equation has all its variables assigned, it will not be modified in the subsequent calls of the assume method until some of the variable values are retracted with the backtrack method. And when this happens, at least two variables lose their values so the equation stays propagation saturated. As a consequence, the tableau does not have to be modified when backtracking.

4) *Clausal Explanations:* Let us study how the clausal explanations for xor-conflicts (step 2 in assume) and xor-implied literals (step 5) are obtained.

- Under the reasonable assumption that the CNF solver does not make contradictory truth assignments, an xor-conflict can only happen when the xor-assumption  $x \equiv v$  is an xor-implied literal derived earlier but ignored so far for some scheduling reason by the CNF-part solver. Thus there is an equation  $x := y_1 \oplus \dots \oplus y_m \oplus p$  in  $\mathcal{E}$  such that  $\tau(x) := \tau(y_1) \oplus \dots \oplus \tau(y_m) \oplus p$  and  $\tau(x) \neq v$ ; the explanation is now the clause  $\neg(y_1 \equiv \tau(y_1)) \vee \dots \vee \neg(y_m \equiv \tau(y_m)) \vee \neg(x \equiv v)$ .
- For an xor-implied literal  $z \equiv v_z$  derived in step 5, the explanation is simply a clause in the straightforward CNF translation of the equation, i.e.  $\neg(x \equiv \tau(x)) \vee \neg(x'_1 \equiv \tau(x'_1)) \vee \dots \vee \neg(x'_m \equiv \tau(x'_m)) \vee (z \equiv v_z)$ .

## C. Implementation

Our implementation of the incremental Gauss-Jordan xor-reasoning module uses a dense matrix representation where one element in the matrix uses one bit of memory. The xor-reasoning module maintains two such matrices. In the first matrix the rows are consecutively in the memory, and in the second the columns are consecutively in the memory. The first matrix allows efficient implementation for row operations and the second matrix for efficient pivoting. To detect xor-implied literals, each row is associated with a counter tracking the number of unassigned variables. When this counter is one (or zero), an xor-implied literal (or a potential conflict) is available. Upon backtracking it suffices to restore the counters tracking unassigned variables. Gauss-Jordan xor-reasoning module is only used after unit propagation is saturated. To strengthen unit propagation over xor-constraints, explanations for xor-implied literals are added as learned xor-constraints.

## D. Experimental Evaluation

To evaluate the effect of incremental Gauss-Jordan elimination in the DPLL(XOR) framework, we integrated three xor-reasoning modules with different deduction engines (unit propagation, equivalence reasoning, Gauss-Jordan) to minisat 2.0 core. In this experiment, we focus on the domain of logical cryptanalysis by modeling a known-plaintext attack on stream cipher Trivium. The task is to recover the full 80-bit key when the IV and a number of cipher stream bits (8 to 16) are given. All instances are satisfiable and it is likely that a number of keys produce the same given prefix of the cipher stream. Figure 1 shows how unit propagation, equivalence reasoning, incremental Gauss-Jordan and cryptominisat 2.9.2 perform on these instances. The strength of the deduction

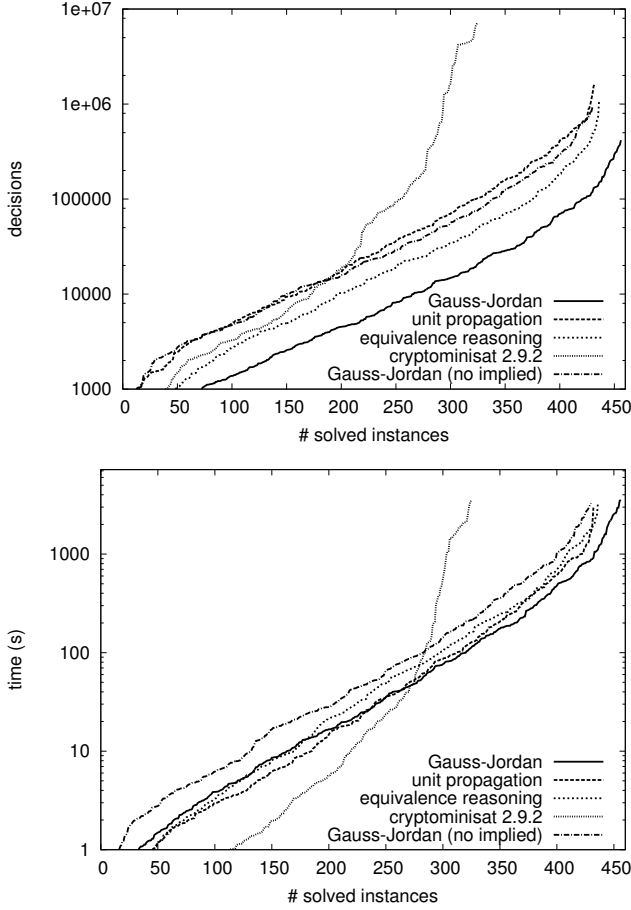


Fig. 1. Comparison of three xor-reasoning modules (unit propagation, equivalence reasoning, Gauss-Jordan) and cryptominisat 2.9.2 on Trivium

engine is well reflected in the results. The solver configuration relying only on unit propagation requires the most decisions. Equivalence reasoning gives a significant reduction in the number of decisions and enables the solver to solve more instances. The solver configuration using incremental Gauss-Jordan solves the highest number of instances and using fewest number of decisions. Considering the solving time, unit propagation can be implemented very efficiently, so easier instances are solved fastest using plain unit propagation. Equivalence reasoning incurs an additional computational overhead which causes it to perform slower than unit propagation despite the reduction in the number of decisions. Incremental Gauss-Jordan is computationally intensive but the reduction in the number of decisions is large enough to make it scale better for the harder instances. To illustrate the effect of xor-implied literals deduced by Gauss-Jordan, a solver configuration using Gauss-Jordan only to detect conflicts and otherwise resorting to unit propagation is included in the comparison. Detecting conflicts as early as possible does not seem to help on this benchmark. The lack of performance of cryptominisat 2.9.2 is probably due to differences in restart policies or other heuristics. Gaussian elimination as implemented in cryptominisat 2.9.2 using row echelon form does not seem to be very useful

in this benchmark because on majority of the instances it does not detect conflicts earlier nor give any xor-implied literals.

#### IV. EXPLOITING BICONNECTED COMPONENTS

When using a dense representation for matrices in the xor-reasoning modules based on Gauss or Gauss-Jordan elimination, the worst-case memory use is  $\mathcal{O}(ne)$ , where  $n$  is the number of variables and  $e$  the number of linearly independent xor-constraints in  $\phi_{\text{xor}}$ . Naturally, when the xor-part  $\phi_{\text{xor}}$  can be decomposed into variable-disjoint sets of xor-constraints (connected components of the constraint graph formally defined below), each such set can be handled by a separate xor-reasoning module with smaller memory requirements. When using a sparse matrix representation, the memory usage does not improve with such a connected component decomposition.

We now give an improved decomposition technique that is based on a new decomposition theorem stating that, in order to guarantee full propagation, it is enough to (i) propagate only values through “cut variables”, and (ii) have full propagation for the “biconnected components” between the cut variables. Thus equivalences and more complicated relationships between variables in different biconnected components do not have to be considered and each component can be handled by a separate xor-reasoning module.

Formally, given an xor-constraint conjunction  $\phi_{\text{xor}}$ , we define that a *cut variable* is a variable  $x \in \text{vars}(\phi_{\text{xor}})$  for which there is a partition  $(V_a, V_b)$  of xor-constraints in  $\phi_{\text{xor}}$  with  $\text{vars}(V_a) \cap \text{vars}(V_b) = \{x\}$ ; such a partition  $(V_a, V_b)$  is called an *x-cut partition* of  $\phi_{\text{xor}}$ . The *biconnected components* of  $\phi_{\text{xor}}$  are defined to be the equivalence classes in the reflexive and transitive closure of the relation  $\{(D, E) \mid D \text{ and } E \text{ share a non-cut variable}\}$  over the xor-constraints in  $\phi_{\text{xor}}$ .

*Example 7:* Let  $\phi_{\text{xor}} = (a \oplus b \oplus c \equiv \top) \wedge (b \oplus d \oplus e \equiv \top) \wedge (c \oplus e \equiv \top) \wedge (d \oplus e \oplus f \equiv \perp) \wedge (f \oplus g \oplus h \equiv \top) \wedge (h \oplus i \oplus j \equiv \perp) \wedge (i \oplus j \oplus k \equiv \top) \wedge (f \oplus l \oplus m \equiv \top) \wedge (l \oplus n \oplus o \equiv \perp)$ . The cut variables of  $\phi_{\text{xor}}$  are  $f, h$  and  $l$ . Thus its five biconnected components are (i)  $\{(a \oplus b \oplus c \equiv \top), (b \oplus d \oplus e \equiv \top), (c \oplus e \equiv \top), (d \oplus e \oplus f \equiv \perp)\}$ , (ii)  $\{(f \oplus g \oplus h \equiv \top)\}$ , (iii)  $\{(h \oplus i \oplus j \equiv \perp), (i \oplus j \oplus k \equiv \top)\}$ , (iv)  $\{(f \oplus l \oplus m \equiv \top)\}$ , and (v)  $\{(l \oplus n \oplus o \equiv \perp)\}$ .

Cut variables and biconnected components are probably best illustrated by means of constraint graphs. Such graphs also give us a method for computing the cut variables, and consequently also the biconnected components. The *constraint graph* of an xor-constraint conjunction  $\phi_{\text{xor}}$  is a labeled bipartite graph  $G = \langle V, E, L \rangle$ , where

- the set of vertices  $V$  is the disjoint union of (i) *variable vertices*  $V_{\text{vars}} = \text{vars}(\phi_{\text{xor}})$  which are graphically represented with circles, and (ii) *constraint vertices*  $V_{\text{constrs}} = \{D \mid D \text{ is an xor-constraint in } \phi_{\text{xor}}\}$  drawn as rectangles,
- $E = \{\{x, D\} \mid x \in V_{\text{vars}} \wedge D \in V_{\text{constrs}} \wedge x \in \text{vars}(D)\}$  are the edges connecting the variables and the xor-constraints in which they occur, and
- $L$  labels each xor-constraint vertex  $(x_1 \oplus \dots \oplus x_k \equiv p)$  with the parity  $p$ .

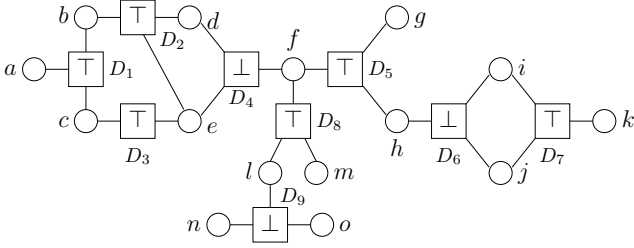


Fig. 2. The constraint graph of the conjunction  $\phi_{xor}$  in Ex. 7

As usual for graphs, (i) a *connected component* of constraint graph  $G$  is a maximal connected subgraph of  $G$ , (ii) a *cut vertex* of  $G$  is a vertex in it whose removal will break a connected component of  $G$  into two or more connected components, and (iii) a *biconnected component* of  $G$  is a maximal biconnected subgraph (a graph is biconnected if it is connected and removing any vertex leaves the graph connected).

*Example 8:* The constraint graph of the conjunction  $\phi_{xor}$  in Ex. 7 is shown in Fig. 2. The cut vertices of it are  $D_1$ ,  $D_4$ ,  $f$ ,  $D_5$ ,  $h$ ,  $D_6$ ,  $D_7$ ,  $D_8$ ,  $l$ , and  $D_9$ . Its biconnected components are the subgraphs induced by the vertex sets  $\{a, D_1\}$ ,  $\{D_1, b, D_2, d, c, D_3, e, D_4\}$ ,  $\{D_4, f\}$ , and so on. Observe that the biconnected components are not vertex-disjoint.

We see that, due to the presense of the vertices for the xor-constraints, the biconnected components of a constraint graph  $G$  for  $\phi_{xor}$  do not directly correspond to the biconnected components of  $\phi_{xor}$ . However, the cut vertices of  $G$ , when restricted to variable vertices, correspond exactly to the cut variables of  $\phi_{xor}$ . Therefore, we have a linear time algorithm for computing the biconnected components of  $\phi_{xor}$ :

- 1) Build (implicitly) the constraint graph  $G$  for  $\phi_{xor}$ .
- 2) Use an algorithm by Hopcroft and Tarjan [19] to compute the biconnected components of  $G$  in linear time; as a byproduct, one gets all the cut vertices and thus the cut variables as well.
- 3) Build the biconnected components of  $\phi_{xor}$  by putting two xor-constraints in the same component if they share a non-cut variable.

#### A. How to Exploit

As biconnected components are connected to each other only through cut variables, in the DPLL(XOR) framework we can actually handle them by separate xor-reasoning modules. In this setting a value for a cut variable deduced by some xor-reasoning module is communicated back to the CNF-part solver as an xor-implied literal, and the CNF-part solver then gives the value as an xor-assumption to the other xor-reasoning modules. Based on the following theorem, we see that this kind of decomposition of  $\phi_{xor}$  preserves full propagation in the following sense: if the modules can provide full propagation for each of the components, then full propagation is achieved for the whole xor-part  $\phi_{xor}$ , too. Basically the theorem states that only cut variable values, not equivalences or more complex relationships, have to be communicated

between biconnected components. For relating the theorem to biconnected components, see the example after the theorem and observe that if  $(V_a, V_b)$  is an  $x$ -cut partition of  $\phi_{xor}$ , then  $V_a$  and  $V_b$  are (disjoint) unions of one or more biconnected components of  $\phi_{xor}$ .

*Theorem 4:* Let  $(V_a, V_b)$  be an  $x$ -cut partition of  $\phi_{xor}$ . Let  $\phi_{xor}^a = \bigwedge_{D \in V_a} D$ ,  $\phi_{xor}^b = \bigwedge_{D \in V_b} D$ , and  $\tilde{l}_1, \dots, \tilde{l}_k, \hat{l} \in \text{lits}(\phi_{xor})$ . Then it holds that:

- If  $\phi_{xor} \wedge \tilde{l}_1 \wedge \dots \wedge \tilde{l}_k$  is unsatisfiable, then
  - 1)  $\phi_{xor}^a \wedge \tilde{l}_1 \wedge \dots \wedge \tilde{l}_k$  or  $\phi_{xor}^b \wedge \tilde{l}_1 \wedge \dots \wedge \tilde{l}_k$  is unsatisfiable; or
  - 2)  $\phi_{xor}^a \wedge \tilde{l}_1 \wedge \dots \wedge \tilde{l}_k \models (x \equiv p_x)$  and  $\phi_{xor}^b \wedge \tilde{l}_1 \wedge \dots \wedge \tilde{l}_k \models (x \equiv p_x \oplus \top)$  for some  $p_x \in \{\perp, \top\}$ .
- If  $\phi_{xor} \wedge \tilde{l}_1 \wedge \dots \wedge \tilde{l}_k$  is satisfiable and  $\phi_{xor} \wedge \tilde{l}_1 \wedge \dots \wedge \tilde{l}_k \models \hat{l}$ , then
  - 1)  $\phi_{xor}^a \wedge \tilde{l}_1 \wedge \dots \wedge \tilde{l}_k \models \hat{l}$  or  $\phi_{xor}^b \wedge \tilde{l}_1 \wedge \dots \wedge \tilde{l}_k \models \hat{l}$ ; or
  - 2)  $\phi_{xor}^a \wedge \tilde{l}_1 \wedge \dots \wedge \tilde{l}_k \models (x \equiv p_x)$  and  $\phi_{xor}^b \wedge \tilde{l}_1 \wedge \dots \wedge \tilde{l}_k \wedge (x \equiv p_x) \models \hat{l}$ ; or
  - 3)  $\phi_{xor}^b \wedge \tilde{l}_1 \wedge \dots \wedge \tilde{l}_k \models (x \equiv p_x)$  and  $\phi_{xor}^a \wedge \tilde{l}_1 \wedge \dots \wedge \tilde{l}_k \wedge (x \equiv p_x) \models \hat{l}$ .

*Example 9:* Take again the conjunction  $\phi_{xor}$  in Ex. 7, illustrated in Fig. 2. Assume the xor-assumptions  $b, \neg g$ , and  $o$ ; now  $\phi_{xor} \wedge b \wedge \neg g \wedge o \models \neg k$ . We can deduce this in a biconnected component-wise manner as follows. First, consider the  $f$ -cut partition  $(\{D_1, \dots, D_4\}, \{D_5, \dots, D_9\})$ . Now  $D_1 \wedge \dots \wedge D_4 \wedge b \models \neg f$  and  $D_5 \wedge \dots \wedge D_9 \wedge \neg g \wedge o \wedge \neg f \models \neg k$ . For  $D_5 \wedge \dots \wedge D_9 \wedge \neg g \wedge o \wedge \neg f \models \neg k$  we apply the theorem again by considering the  $f$ -cut partition  $(\{D_8, D_9\}, \{D_5, D_6, D_7\})$  of  $D_5 \wedge \dots \wedge D_9$ : now  $D_5 \wedge D_6 \wedge D_7 \wedge \neg g \wedge \neg f \models \neg k$  and thus the biconnected components  $\{D_8\}$  and  $\{D_9\}$  are not needed in the derivation. For  $D_5 \wedge D_6 \wedge D_7 \wedge \neg g \wedge \neg f \models \neg k$ , we apply the theorem again by considering the  $h$ -cut partition  $(\{D_5\}, \{D_6, D_7\})$ :  $D_5 \wedge \neg g \wedge \neg f \models h$  and  $D_6 \wedge D_7 \wedge h \models \neg k$ . Thus we can derive  $\neg k$  from  $\phi_{xor} \wedge b \wedge \neg g$  in a component-by-component fashion.

We observe the following: some biconnected components can be singleton sets. For such components we can provide full propagation easily by the basic unit propagation. These singleton components originate from “tree-like” parts of  $\phi_{xor}$ : the trees can be “outermost” (constraints  $D_8$  and  $D_9$  in Fig. 2) or between two non-tree-like components ( $D_5$  in Fig. 2). Thus our new result in a sense subsumes one in [20], where we suggested clausification of “outermost” tree-like parts.

#### B. Experimental Evaluation

To evaluate the relevance of detecting biconnected components, we studied the benchmark instances in “crafted” and “industrial/application” categories of the SAT Competitions 2005, 2007, and 2009 as well as all the instances in the SAT Competition 2011 (available at <http://www.satcompetition.org/>). To get rid of some “trivial” xor-constraints, we eliminated unary clauses and binary xor-constraints from each instance by unit propagation and substitution, respectively. After this easy preprocessing, 474 instances (with some duplicates due to overlap in the competitions) having xor-constraints

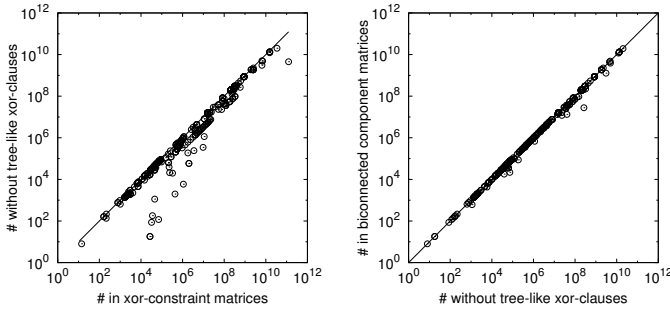


Fig. 3. Reduction in memory usage for dense matrix representation when (i) tree-like xor-constraints are removed (ii) only biconnected components are counted in SAT 2005-2011 competition instances. In the latter case, although the difference seems negligible in logarithmic scale, the memory consumption is reduced by additional 13.5% on average in 110 instances having multiple biconnected components.

remained. We first examine how the memory usage can be improved by removing (i) tree-like xor-constraints and (ii) storing each biconnected component in a separate matrix. Figure 3 shows the reduction in memory usage when using dense matrix representation to store the xor-constraints. As already reported in [20], a significant proportion of xor-constraints in these competition instances are tree-like and performing additional reasoning beyond unit propagation cannot be used to detect more implied literals. Removing these tree-like xor-constraints from Gauss-Jordan matrices reduces the memory usage greatly. An additional reduction in memory usage is obtained by storing each biconnected component in a separate matrix.

We ran minisat 2.0 core augmented with four different xor-reasoning modules (unit propagation, equivalence reasoning, Gauss-Jordan, and a variant of Gauss-Jordan exploiting biconnected components) and cryptominisat 2.9.2 on these instances. Figure 4 shows the number of instances solved with respect to the number of heuristic decisions. Unit propagation and equivalence reasoning perform similarly on these instances. Incremental Gauss-Jordan solves a substantial number of the instances almost instantly and also manages to solve more instances in total. The solver cryptominisat 2.9.2 performs very well on these instances. Figure 4 also shows the number of instances solved with respect to time. Since equivalence reasoning does not reduce the number of decisions, the computational overhead is reflected in the slowest solving time. Incremental Gauss-Jordan is computationally more intensive but complete parity reasoning pays off on these instances leading to fastest solving compared to our other xor-reasoning modules. Omitting tree-like xor-constraints from Gauss-Jordan matrices and splitting biconnected components into separate matrices offers a significant reduction in the solving time without sacrificing completeness of reasoning. To illustrate the effect of implied literals deduced by Gauss-Jordan, we also ran a solver using Gauss-Jordan only to detect conflicts and otherwise resorting to unit propagation. More instances are solved and faster when all implied literals are deduced.

Biconnected components may be exploited even without

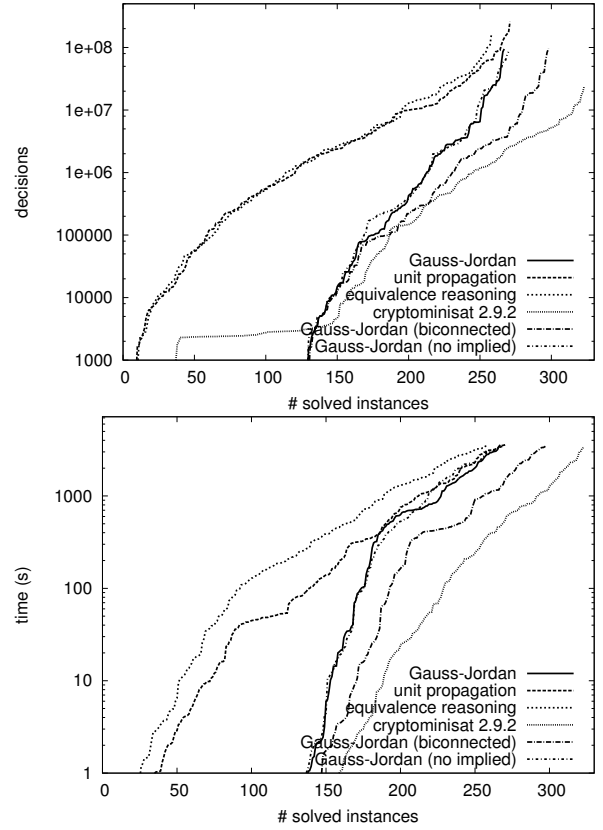


Fig. 4. Number of SAT 2005-2011 competition instances solved w.r.t. decisions and time

modifying the solver. The solver cryptominisat accepts a mixture of clauses and xor-constraints as its input. When Gaussian elimination is used, the solver stores each connected component in a separate matrix. By translating each singleton biconnected component into CNF, some non-trivial biconnected components may become connected components and are then placed into separate matrices improving memory usage. We considered the 110 SAT competition instances with multiple biconnected components and found 60 instances where some biconnected components could be separated by translating singleton biconnected components to CNF. Figure 5 shows the effect of the translation in the number of decisions and solving time. The solver cryptominisat 2.9.2 solves 44 of the unmodified instances. After the translation, cryptominisat 2.9.2 is able to solve 50 instances and slightly faster.

## V. ELIMINATING XOR-INTERNAL VARIABLES

A cnf-xor formula  $\phi_{\text{or}} \wedge \phi_{\text{xor}}$  may have *xor-internal* variables occurring only in  $\phi_{\text{xor}}$ . As suggested in [11], such variables can be eliminated from the formula by substituting them with their “definitions”; e.g. if  $x_1 \oplus x_2 \oplus x_3 \equiv \top$  is an xor-constraint where  $x_1$  is an xor-internal variable, then remove the parity constraint and replace every occurrence of  $x_1$  in all the other parity constraints by  $x_2 \oplus x_3 \oplus \top$ . When using dense matrix representation, the matrices can be made more compact by eliminating xor-internal variables. For instance, one of our

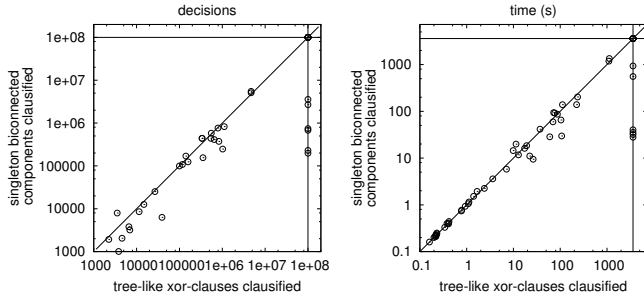


Fig. 5. Effect in decisions and solving time for cryptominisat when singleton biconnected components in SAT competition instances are translated to CNF

Trivium benchmark instances has 5900 xor-internal variables out of 11484 variables and 8590 parity constraints in two connected components. The total number of elements in the matrices is  $55 \times 10^6$  elements. By eliminating all xor-internal variables this can be reduced to  $8 \times 10^6$  elements. The instance has three biconnected components (as all of our Trivium instances) and storing them in separate matrices requires  $33 \times 10^6$  elements in total. But, if a cut variable connecting the biconnected components is xor-internal, it is eliminated and the two biconnected components are merged into one bigger biconnected component. To preserve biconnected components, only the variables occurring in a single biconnected component and not in the CNF-part should be eliminated. There are 5906 such variables in the instances and after the elimination the total number of elements in three matrices is  $5 \times 10^6$ . Figure 6 shows the effect of eliminating such variables in our Trivium instances. Unit propagation benefits from elimination of xor-internal variables. Fewer watched literals (variables) are needed for longer xor-constraints to detect when an implied literal can be deduced. The solver configuration using incremental Gauss-Jordan elimination manages to solve all of our benchmark instances with reduced solving time.

#### ACKNOWLEDGMENT

This work has been financially supported by the Academy of Finland under the Finnish Centre of Excellence in Computational Inference (COIN).

#### REFERENCES

- [1] J. Marques-Silva, I. Lynce, and S. Malik, "Conflict-driven clause learning SAT solvers," in *Handbook of Satisfiability*. IOS Press, 2009.
- [2] A. Urquhart, "Hard examples for resolution," *Journal of the ACM*, vol. 34, no. 1, pp. 209–219, 1987.
- [3] C. M. Li, "Integrating equivalency reasoning into Davis-Putnam procedure," in *Proc. AAAI/IAAI 2000*. AAAI Press, 2000, pp. 291–296.
- [4] —, "Equivalency reasoning to solve a class of hard SAT problems," *Information Processing Letters*, vol. 76, no. 1–2, pp. 75–81, 2000.
- [5] P. Baumgartner and F. Massacci, "The taming of the (X)OR," in *Proc. CL 2000*, ser. LNCS, vol. 1861. Springer, 2000, pp. 508–522.
- [6] C. M. Li, "Equivalent literal propagation in the DLL procedure," *Discrete Applied Mathematics*, vol. 130, no. 2, pp. 251–276, 2003.
- [7] M. Heule and H. van Maaren, "Aligning CNF- and equivalence-reasoning," in *Proc. SAT 2004*, ser. LNCS, vol. 3542. Springer, 2004, pp. 145–156.
- [8] M. Heule, M. Dufour, J. van Zwieten, and H. van Maaren, "March\_eq: Implementing additional reasoning into an efficient look-ahead SAT solver," in *Proc. SAT 2004*, ser. LNCS, vol. 3542. Springer, 2004, pp. 345–359.

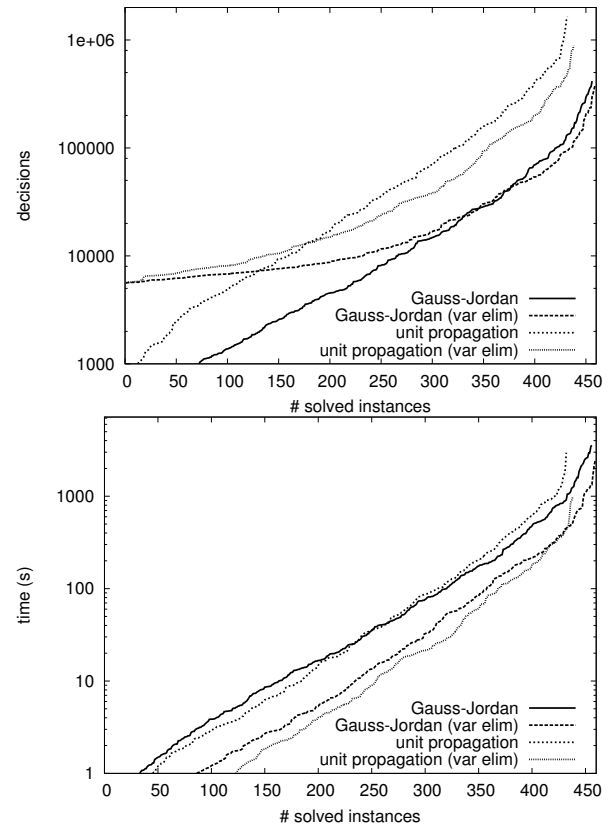


Fig. 6. Effect of eliminating xor-internal variables while preserving biconnected components in the number of decisions and solving time on Trivium

- [9] J. Chen, "Building a hybrid SAT solver via conflict-driven, look-ahead and XOR reasoning techniques," in *Proc. SAT 2009*, ser. LNCS, vol. 5584. Springer, 2009, pp. 298–311.
- [10] M. Soos, K. Nohl, and C. Castelluccia, "Extending SAT solvers to cryptographic problems," in *Proc. SAT 2009*, ser. LNCS, vol. 5584. Springer, 2009, pp. 244–257.
- [11] T. Laitinen, T. Junttila, and I. Niemelä, "Extending clause learning DPLL with parity reasoning," in *Proc. ECAI 2010*. IOS Press, 2010, pp. 21–26.
- [12] M. Soos, "Enhanced gaussian elimination in DPLL-based SAT solvers," in *Pragmatics of SAT*, Edinburgh, Scotland, GB, July 2010, pp. 1–1.
- [13] T. Laitinen, T. Junttila, and I. Niemelä, "Equivalence class based parity reasoning with DPLL(XOR)," in *Proc. ICTAI 2011*. IEEE, 2011, pp. 649–658.
- [14] —, "Conflict-driven XOR-clause learning," in *Proc. SAT 2012*, ser. LNCS, vol. 7317. Springer, 2012, pp. 383–396.
- [15] C.-S. Han and J.-H. R. Jiang, "When boolean satisfiability meets gaussian elimination in a simplex way," in *Proc. CAV 2012*, 2012, to appear.
- [16] R. Nieuwenhuis, A. Oliveras, and C. Tinelli, "Solving SAT and SAT modulo theories: From an abstract Davis-Putnam-Logemann-Loveland procedure to DPLL(T)," *Journal of the ACM*, vol. 53, no. 6, pp. 937–977, 2006.
- [17] C. Barrett, R. Sebastiani, S. A. Seshia, and C. Tinelli, "Satisfiability modulo theories," in *Handbook of Satisfiability*. IOS Press, 2009.
- [18] B. Dutertre and L. M. de Moura, "A fast linear-arithmetic solver for DPLL(T)," in *CAV*, ser. LNCS, vol. 4144. Springer, 2006, pp. 81–94.
- [19] J. E. Hopcroft and R. E. Tarjan, "Efficient algorithms for graph manipulation [h] (algorithm 447)," *Communications of the ACM*, vol. 16, no. 6, pp. 372–378, 1973.
- [20] T. Laitinen, T. Junttila, and I. Niemelä, "Classifying and propagating parity constraints," 2012, accepted for publication in CP 2012.



## APPENDIX

In this appendix, we provide proofs for the Lemmas and Theorems in the paper. Before the actual proofs, we provide some auxiliary results.

For two xor-constraints  $D = (x_1 \oplus \dots \oplus x_k \equiv p)$  and  $E = (y_1 \oplus \dots \oplus y_l \equiv q)$ , we define their linear combination xor-constraint by  $D + E = (x_1 \oplus \dots \oplus x_k \oplus y_1 \oplus \dots \oplus y_l \equiv p \oplus q)$ . Some fundamental, easy to verify properties are  $D + D + E = E$ ,  $D \wedge E \models D + E$ ,  $D \wedge E \models D \wedge (D + E)$ , and  $D \wedge (D + E) \models D \wedge E$ . Furthermore, the logical consequence xor-constraints of a conjunction  $\phi_{\text{xor}}$  are exactly those that are linear combinations of the xor-constraints in  $\phi_{\text{xor}}$ :

*Lemma 5:* Let  $\psi$  be a conjunction of xor-constraints. Now  $\psi$  is unsatisfiable if and only if there is a subset  $S$  of xor-constraints in  $\psi$  such that  $\sum_{D \in S} D = (\perp \equiv \top)$ . If  $\psi$  is satisfiable and  $E$  is an xor-constraint, then  $\psi \models E$  if and only if there is a subset  $S$  of xor-constraints in  $\psi$  such that  $\sum_{D \in S} D = E$ .

*Proof:* There are two cases to consider.

- Case I:  $\psi$  is unsatisfiable.

If there is a subset  $S$  of xor-constraints in  $\psi$  such that  $\sum_{D \in S} D = (\perp \equiv \top)$ , then, by iteratively applying  $D_1 \wedge D_2 \models D_1 + D_2$ , we have  $\bigwedge_{D \in S} D \models \sum_{D \in S} D$ , i.e.  $\sum_{D \in S} D \models (\perp \equiv \top)$ , and thus  $\psi$  is unsatisfiable. For the other direction, assume that  $\psi$  is unsatisfiable. Represent the conjunction  $\psi$  as a system of linear equations modulo two in matrix form. Gaussian elimination must result in an equation  $0 \equiv 1 \pmod{2}$  in some row  $r$  of the matrix. The row  $r$  is a linear combination of some original rows  $r_1, \dots, r_n$ . Each original row  $r_i$  corresponds to a distinct xor-constraint  $C(r_i)$  in  $\psi$ . Thus,  $S = \{C(r_1), \dots, C(r_n)\} \subseteq \psi$  is a subset of xor-constraints in  $\psi$  such that  $\sum_{D \in S} D = (\perp \equiv \top)$ .

- Case II:  $\psi$  is satisfiable.

If there is a subset  $S$  of xor-constraints in  $\psi$  such that  $\sum_{D \in S} D = E$ , then, by iteratively applying  $D_1 \wedge D_2 \models D_1 + D_2$ , we have  $\bigwedge_{D \in S} D \models \sum_{D \in S} D$  and thus  $\bigwedge_{D \in S} D \models E$  and  $\psi \models E$ .

Assume that  $\psi \models E$ . We have  $\emptyset \neq \text{vars}(E) \subseteq \text{vars}(\psi)$ . Create a (reduced row echelon form) tableau  $\mathcal{E}$  for  $\psi$  with the following property holding for each equation  $e$ : if  $e$  has a non-basic variable occurring in  $E$ , then the basic variable of  $e$  also occurs in  $E$ . Such a tableau can be obtained by applying the swap operator at most  $|\text{vars}(E)|$  times to a tableau for  $\psi$ . By construction, each equation  $e$  of form  $x := x_1 \oplus \dots \oplus x_k \oplus p$  in  $\mathcal{E}$  corresponds to a linear combination  $C_e = (x \oplus x_1 \oplus \dots \oplus x_k \equiv p)$  of a subset  $S_e$  of xor-constraints in  $\psi$ . Consider the linear combination  $E' = \sum_{e \in \mathcal{E} \wedge \text{vars}(e) \cap \text{vars}(E) \neq \emptyset} C_e$  of equations in  $\mathcal{E}$  having at least one common variable with  $E$ . It holds that  $\psi \models E'$ . As  $\psi \models E$  and  $\psi \models E'$ , it also holds that  $\psi \models E \wedge E'$  and thus  $\psi \models E + E'$ . We have three cases to consider:

- Case A:  $E + E' = (\perp \equiv \top)$ . This is not possible as  $\psi$  would be unsatisfiable.

- Case B:  $E + E' = (\perp \equiv \perp)$ . Now  $E'$  is equal to  $E$ . Thus there is a subset  $S$  of xor-constraints in  $\psi$  such that  $\sum_{D \in S} D = E$ , namely the ones that appear an odd number of times in  $\bigcup_{e \in \mathcal{E} \wedge \text{vars}(e) \cap \text{vars}(E) \neq \emptyset} S_e$  (whose linear combination  $E'$  is).
- Case C:  $E + E'$  is  $y_1 \oplus \dots \oplus y_k \equiv p$  with  $k \geq 1$ . All the variables  $y_1, \dots, y_k$  must be non-basic variables in  $\mathcal{E}$  because (i) all the basic variables of  $\mathcal{E}$  occurring in  $E$  also occur in  $E'$ , and (ii) the basic variables of  $\mathcal{E}$  not occurring in  $E$  are not included in  $E'$  either. But because  $y_1, \dots, y_k$  are non-basic variables, we can build the following satisfying truth assignment  $\tau$  for  $\psi$ : (i) assign  $y_1, \dots, y_k$  some values such that that  $\tau(y_1) \oplus \dots \oplus \tau(y_k) \neq p$ , (ii) assign the other non-basic variables in  $\mathcal{E}$  with arbitrary values, and (iii) evaluate the values of the basic variables. Thus it is not possible that  $\psi \models (y_1 \oplus \dots \oplus y_k \equiv p)$  and the case of  $E + E'$  equaling to  $y_1 \oplus \dots \oplus y_k \equiv p$  is impossible. ■

Another key property of tableaux is that the equations in them are logical consequences of the represented conjunction of xor-constraints:

*Fact 6:* If  $\mathcal{E}$  is a tableau for  $\phi_{\text{xor}}$ , then  $x_i := x_{i,1} \oplus \dots \oplus x_{i,k_i} \oplus p_i \in \mathcal{E}$  implies  $\phi_{\text{xor}} \models (x_i \oplus x_{i,1} \oplus \dots \oplus x_{i,k_i} \equiv p_i)$ .

### A. Proof of Lemma 1

*Lemma 1:* Let  $\langle \mathcal{E}, \tau \rangle$  be a propagation saturated assigned tableau for  $\phi_{\text{xor}}$ . The formula  $\phi_{\text{xor}} \wedge \bigwedge_{(x \mapsto v) \in \tau} (x \equiv v)$  is satisfiable if and only if  $\langle \mathcal{E}, \tau \rangle$  is consistent.

*Proof:* First, assume that  $\langle \mathcal{E}, \tau \rangle$  is consistent. Extend the assignment  $\tau$  into a total one  $\tau'$  by (i) assigning arbitrary values to the unassigned non-basic variables, and (ii) evaluating the unassigned basic variables according to their equations. As  $\langle \mathcal{E}, \tau \rangle$  is propagation saturated and consistent, the resulting truth assignment  $\tau'$  does not violate any of the equations. Because  $\bigwedge_{x_i := x_{i,1} \oplus \dots \oplus x_{i,k_i} \oplus p_i \in \mathcal{E}} (x_i \oplus x_{i,1} \oplus \dots \oplus x_{i,k_i} \equiv p_i)$  is logically equivalent to  $\phi_{\text{xor}}$ , formula  $\phi_{\text{xor}} \wedge \bigwedge_{(x \mapsto v) \in \tau} (x \equiv v)$  is satisfied by  $\tau'$ .

Now, assume that  $\langle \mathcal{E}, \tau \rangle$  is inconsistent. Then there is an equation  $x_i := x_{i,1} \oplus \dots \oplus x_{i,k_i} \oplus p_i$  such that  $\tau(x)$  is defined for all  $x \in \{x_i, x_{i,1}, \dots, x_{i,k_i}\}$  and  $\tau(x_i) \neq \tau(x_{i,1}) \oplus \dots \oplus \tau(x_{i,k_i}) \oplus p_i$ . By Fact. 6,  $\phi_{\text{xor}} \models (x_i \oplus x_{i,1} \oplus \dots \oplus x_{i,k_i} \equiv p_i)$ . Now  $\tau$  or any of its extensions do not satisfy  $(x_i \oplus x_{i,1} \oplus \dots \oplus x_{i,k_i} \equiv p_i)$ ; thus  $\tau$  or any of its extensions do not satisfy  $\phi_{\text{xor}}$  either. As a result, the formula  $\phi_{\text{xor}} \wedge \bigwedge_{(x \mapsto v) \in \tau} (x \equiv v)$  is unsatisfiable. ■

### B. Proof of Lemma 2

*Lemma 2:* Let  $\langle \mathcal{E}, \tau \rangle$  be a consistent, propagation saturated assigned tableau for  $\phi_{\text{xor}}$ . For each literal  $y \equiv v_y$  it holds that  $\phi_{\text{xor}} \wedge \bigwedge_{(x \mapsto v_x) \in \tau} (x \equiv v_x) \models (y \equiv v_y)$  if and only if  $\tau(y) = v_y$ .

*Proof:* If  $\tau(y) = v_y$ , then  $\phi_{\text{xor}} \wedge \bigwedge_{(x \mapsto v_x) \in \tau} (x \equiv v_x) \models (y \equiv v_y)$  holds trivially as  $(y \mapsto v_y) \in \tau$ .

Assume that  $\phi_{\text{xor}} \wedge \bigwedge_{(x \mapsto v_x) \in \tau} (x \equiv v_x) \models (y \equiv v_y)$  holds. As  $\langle \mathcal{E}, \tau \rangle$  is consistent and propagation saturated, by Lemma 1  $\phi_{\text{xor}} \wedge \bigwedge_{(x \mapsto v_x) \in \tau} (x \equiv v_x)$  is satisfiable. Suppose that  $\mathcal{E}$  has  $n$  non-basic variables not assigned by  $\tau$ . As  $\langle \mathcal{E}, \tau \rangle$  is consistent and propagation saturated, there are  $2^n$  total extensions of  $\tau$  that respect the equations in  $\mathcal{E}$ , obtained by assigning arbitrary values to the unassigned non-basic variables and then evaluating the unassigned basic variables. All these extensions satisfy  $\phi_{\text{xor}} \wedge \bigwedge_{(x \mapsto v_x) \in \tau} (x \equiv v_x)$ . For each  $\tau$ -unassigned variable  $y$  there is thus at least one satisfying truth assignment where  $y$  is  $\perp$  and one where  $y$  is  $\top$ . Thus  $\phi_{\text{xor}} \wedge \bigwedge_{(x \mapsto v_x) \in \tau} (x \equiv v_x) \models (y \equiv v_y)$  can hold only if  $y$  is assigned by  $\tau$  and  $\tau(y) = v_y$ . ■

### C. Proof of Lemma 3

*Lemma 3:* Let  $\langle \mathcal{E}, \tau \rangle$  be a consistent, propagation saturated assigned tableau for  $\phi_{\text{xor}}$ . For any two distinct variables  $y, z$  and any  $p \in \mathbb{B}$ , it holds that  $\phi_{\text{xor}} \wedge \bigwedge_{(x \mapsto v_x) \in \tau} (x \equiv v_x) \models (y \oplus z \equiv p)$  if and only if

- 1)  $\tau(y)$  and  $\tau(z)$  are both defined and  $\tau(y) \oplus \tau(z) = p$ ,
- 2)  $\tau(y)$  and  $\tau(z)$  are undefined and  $\mathcal{E}$  has an equation  $e$  of form  $y := \dots \oplus z \oplus \dots$  such that  $e|_\tau$  is  $y := z \oplus p$ , where  $e|_\tau$  is the equation obtained from  $e$  by substituting the variables in it assigned by  $\tau$  with their values,
- 3)  $\tau(y)$  and  $\tau(z)$  are undefined and  $\mathcal{E}$  has an equation  $e$  of form  $z := \dots \oplus y \oplus \dots$  such that  $e|_\tau$  is  $z := y \oplus p$ , or
- 4)  $\tau(y)$  and  $\tau(z)$  are undefined and  $\mathcal{E}$  has two equations,  $e_y$  and  $e_z$ , of forms  $y := \dots$  and  $z := \dots$  such that  $e_y|_\tau$  is  $y := f$ ,  $e_z|_\tau$  is  $z := g$ , and  $f \oplus g$  equals  $p$ .

*Proof:* Because  $\langle \mathcal{E}, \tau \rangle$  is consistent and propagation saturated, there are  $2^n$  total extensions of  $\tau$  that respect all the equations in  $\mathcal{E}$ , obtained by assigning arbitrary values to the  $n$   $\tau$ -unassigned non-basic variables in  $\langle \mathcal{E}, \tau \rangle$  and then evaluating the  $\tau$ -unassigned basic variables according to the equations. In the following, the set of all such extensions is denoted by  $\Gamma$ . Furthermore, all such total extensions also satisfy  $\phi_{\text{xor}} \wedge \bigwedge_{(x \mapsto v_x) \in \tau} (x \equiv v_x)$  because  $\bigwedge_{x_i := x_{i,1} \oplus \dots \oplus x_{i,k_i} \oplus p_i \in \mathcal{E}} (x_i \oplus x_{i,1} \oplus \dots \oplus x_{i,k_i} \equiv p_i)$  is logically equivalent to  $\phi_{\text{xor}}$ . For the same reason, they are also the only truth assignments over  $\text{vars}(\phi_{\text{xor}})$  that satisfy  $\phi_{\text{xor}} \wedge \bigwedge_{(x \mapsto v_x) \in \tau} (x \equiv v_x)$ . And for each  $\tau$ -unassigned variable  $x$ , there is an extension  $\tau' \in \Gamma$  with  $\tau'(x) = \perp$  and another extension  $\tau'' \in \Gamma$  with  $\tau''(x) = \top$ .

First, assume that  $\tau(y)$  and  $\tau(z)$  are both defined. Now it is straightforward to observe that  $\tau(y) \oplus \tau(z) = p$  if and only if  $\phi_{\text{xor}} \wedge \bigwedge_{(x \mapsto v_x) \in \tau} (x \equiv v_x) \models (y \oplus z \equiv p)$ .

Second, assume that  $\tau(y)$  is defined but  $\tau(z)$  is not (the case when  $\tau(z)$  is defined but  $\tau(y)$  is not is symmetric to this). As  $z$  is  $\tau$ -unassigned, there is a  $\tau' \in \Gamma$  with  $\tau'(z) = \perp$  and a  $\tau'' \in \Gamma$  with  $\tau''(z) = \top$ . As  $\tau'$  and  $\tau''$  also satisfy  $\phi_{\text{xor}} \wedge \bigwedge_{(x \mapsto v_x) \in \tau} (x \equiv v_x)$ ,  $\phi_{\text{xor}} \wedge \bigwedge_{(x \mapsto v_x) \in \tau} (x \equiv v_x) \models (y \oplus z \equiv p)$  cannot hold.

Lastly, assume that  $\tau(y)$  and  $\tau(z)$  are both undefined. We have four cases to consider.

- 1)  $y$  and  $z$  are both non-basic variables. Now there are extensions  $\tau_1, \tau_2, \tau_3, \tau_4 \in \Gamma$  covering all the four truth

value combinations possible for the variable pair  $y$  and  $z$ . As all these also satisfy  $\phi_{\text{xor}} \wedge \bigwedge_{(x \mapsto v_x) \in \tau} (x \equiv v_x)$ ,  $\phi_{\text{xor}} \wedge \bigwedge_{(x \mapsto v_x) \in \tau} (x \equiv v_x) \models (y \oplus z \equiv p)$  cannot hold.

- 2)  $y$  is a basic variable and  $z$  is a non-basic variable.

Take the equation  $e$  of form  $y := \dots$  for  $y$  in  $\mathcal{E}$ . As  $\langle \mathcal{E}, \tau \rangle$  is consistent and propagation saturated, and  $y$  is  $\tau$ -unassigned, there is at least one  $\tau$ -unassigned variable in the right hand side of  $e$ .

If  $e|_\tau$  is  $y := z \oplus p$  for some  $p \in \mathbb{B}$ , i.e. there is exactly one  $\tau$ -unassigned variables in the right hand side of  $e$  and that variable is  $z$ , then the value of  $y$  is fully determined by the value of  $z$  in each  $\tau' \in \Gamma$ , and thus  $\phi_{\text{xor}} \wedge \bigwedge_{(x \mapsto v_x) \in \tau} (x \equiv v_x) \models (y \oplus z \equiv p)$  holds.

On the other hand, if  $\phi_{\text{xor}} \wedge \bigwedge_{(x \mapsto v_x) \in \tau} (x \equiv v_x) \models (y \oplus z \equiv p)$  holds, then the value of  $y$  is fully determined by the value of  $z$  in each  $\tau' \in \Gamma$  and thus  $e|_\tau$  must be  $y := z \oplus p$ .

- 3)  $z$  is a basic variable and  $y$  is a non-basic variable. This case is symmetric to the previous one.
- 4)  $y$  and  $z$  are both basic variables.

If  $\mathcal{E}$  has two equations,  $e_y$  and  $e_z$ , of forms  $y := \dots$  and  $z := \dots$  such that  $e_y|_\tau$  is  $y := f$ ,  $e_z|_\tau$  is  $z := g$ , and  $f \oplus g$  (with duplicate variables eliminated) equals  $p$ , then  $f$  and  $g$  must contain the same variables as otherwise  $f \oplus g$  would not equal  $p$ . Thus  $e_y$  and  $e_z$  must contain the same  $\tau$ -unassigned variables and consequently  $\tau'(y) = \tau'(z) \oplus p$  for each  $\tau' \in \Gamma$ , implying  $\phi_{\text{xor}} \wedge \bigwedge_{(x \mapsto v_x) \in \tau} (x \equiv v_x) \models (y \oplus z \equiv p)$ .

If  $\phi_{\text{xor}} \wedge \bigwedge_{(x \mapsto v_x) \in \tau} (x \equiv v_x) \models (y \oplus z \equiv p)$  holds, then the equations  $e_y$  and  $e_z$  for  $y$  and  $z$ , resp., must contain the same  $\tau$ -unassigned non-basic variables because otherwise there would be extensions  $\tau', \tau'' \in \Gamma$  such that  $\tau'(y) = \tau''(y)$  but  $\tau'(z) \neq \tau''(z)$  and  $\phi_{\text{xor}} \wedge \bigwedge_{(x \mapsto v_x) \in \tau} (x \equiv v_x) \models (y \oplus z \equiv p)$  would not hold. As a consequence,  $e_y|_\tau$  is  $y := f$ ,  $e_z|_\tau$  is  $z := g$ , and  $f \oplus g$  equals  $p$ . ■

### D. Proof of the Decomposition Theorem 4

*Theorem 4:* Let  $(V_a, V_b)$  be an  $x$ -cut partition of  $\phi_{\text{xor}}$ . Let  $\phi_{\text{xor}}^a = \bigwedge_{D \in V_a} D$ ,  $\phi_{\text{xor}}^b = \bigwedge_{D \in V_b} D$ , and  $\tilde{l}_1, \dots, \tilde{l}_k, \hat{l} \in \text{lits}(\phi_{\text{xor}})$ . Then it holds that:

- If  $\phi_{\text{xor}} \wedge \tilde{l}_1 \wedge \dots \wedge \tilde{l}_k$  is unsatisfiable, then
  - 1)  $\phi_{\text{xor}}^a \wedge \tilde{l}_1 \wedge \dots \wedge \tilde{l}_k$  or  $\phi_{\text{xor}}^b \wedge \tilde{l}_1 \wedge \dots \wedge \tilde{l}_k$  is unsatisfiable; or
  - 2)  $\phi_{\text{xor}}^a \wedge \tilde{l}_1 \wedge \dots \wedge \tilde{l}_k \models (x \equiv p_x)$  and  $\phi_{\text{xor}}^b \wedge \tilde{l}_1 \wedge \dots \wedge \tilde{l}_k \models (x \equiv p_x \oplus \top)$  for some  $p_x \in \{\perp, \top\}$ .
- If  $\phi_{\text{xor}} \wedge \tilde{l}_1 \wedge \dots \wedge \tilde{l}_k$  is satisfiable and  $\phi_{\text{xor}} \wedge \tilde{l}_1 \wedge \dots \wedge \tilde{l}_k \models \hat{l}$ , then
  - 1)  $\phi_{\text{xor}}^a \wedge \tilde{l}_1 \wedge \dots \wedge \tilde{l}_k \models \hat{l}$  or  $\phi_{\text{xor}}^b \wedge \tilde{l}_1 \wedge \dots \wedge \tilde{l}_k \models \hat{l}$ ; or
  - 2)  $\phi_{\text{xor}}^a \wedge \tilde{l}_1 \wedge \dots \wedge \tilde{l}_k \models (x \equiv p_x)$  and  $\phi_{\text{xor}}^b \wedge \tilde{l}_1 \wedge \dots \wedge \tilde{l}_k \wedge (x \equiv p_x) \models \hat{l}$ ; or
  - 3)  $\phi_{\text{xor}}^b \wedge \tilde{l}_1 \wedge \dots \wedge \tilde{l}_k \models (x \equiv p_x)$  and  $\phi_{\text{xor}}^a \wedge \tilde{l}_1 \wedge \dots \wedge \tilde{l}_k \wedge (x \equiv p_x) \models \hat{l}$ .

*Proof:* Let  $(V'_a, V'_b)$  be an  $x$ -cut partition of  $\phi_{\text{xor}} \wedge (\tilde{l}_1) \wedge \dots \wedge (\tilde{l}_k)$  with  $\text{vars}(V'_a) = \text{vars}(V_a)$ ,  $\text{vars}(V'_b) = \text{vars}(V_b)$ ,  $V_a \subseteq V'_a$ , and  $V_b \subseteq V'_b$ . Such partition exists because the xor-assumption literals  $\tilde{l}_i$  are unit xor-constraints.

Case I:  $\phi_{\text{xor}} \wedge \tilde{l}_1 \wedge \dots \wedge \tilde{l}_k$  is unsatisfiable. By Lemma 5, there is a subset  $S$  of xor-constraints in  $\phi_{\text{xor}} \wedge (\tilde{l}_1) \wedge \dots \wedge (\tilde{l}_k)$  such that  $\sum_{D \in S} D = (\perp \equiv \top)$ . Observe that  $\sum_{D \in S} D = (\sum_{D \in V'_a \cap S} D) + (\sum_{D \in V'_b \cap S} D)$ . If  $\sum_{D \in V'_a \cap S} D = (\perp \equiv \top)$ , then  $\phi_{\text{xor}}^a \wedge \tilde{l}_1 \wedge \dots \wedge \tilde{l}_k$  is also unsatisfiable. Similarly, if  $\sum_{D \in V'_b \cap S} D = (\perp \equiv \top)$ , then  $\phi_{\text{xor}}^b \wedge \tilde{l}_1 \wedge \dots \wedge \tilde{l}_k$  is unsatisfiable. Otherwise, it must be that  $\sum_{D \in V'_a \cap S} D = (x \equiv p_x)$  and  $\sum_{D \in V'_b \cap S} D = (x \equiv p_x \oplus \top)$  with  $p_x \in \{\perp, \top\}$  because  $V'_a \cap V'_b = \emptyset$ ,  $\text{vars}(V'_a) \cap \text{vars}(V'_b) = \{x\}$  and  $(\sum_{D \in V'_a \cap S} D) + (\sum_{D \in V'_b \cap S} D) = (\perp \equiv \top)$ . Thus  $\phi_{\text{xor}}^a \wedge \tilde{l}_1 \wedge \dots \wedge \tilde{l}_k \models (x \equiv p_x)$  and  $\phi_{\text{xor}}^b \wedge \tilde{l}_1 \wedge \dots \wedge \tilde{l}_k \models (x \equiv p_x \oplus \top)$ .

Case II:  $\phi_{\text{xor}} \wedge \tilde{l}_1 \wedge \dots \wedge \tilde{l}_k$  is satisfiable and  $\phi_{\text{xor}} \wedge \tilde{l}_1 \wedge \dots \wedge \tilde{l}_k \models \hat{l}$  with  $\hat{l} = (y \equiv p_y)$  for some variable  $y$  and  $p_y \in \{\perp, \top\}$ . There is a subset  $S$  of xor-constraints in  $\phi_{\text{xor}} \wedge (\tilde{l}_1) \wedge \dots \wedge (\tilde{l}_k)$  such that  $\sum_{D \in S} D = (y \equiv p_y)$ . Again, observe that  $(\sum_{D \in S} D) = (\sum_{D \in V'_a \cap S} D) + (\sum_{D \in V'_b \cap S} D)$  and thus it must be that either  $y \in \text{vars}(\sum_{D \in V'_a \cap S} D)$  or  $y \in \text{vars}(\sum_{D \in V'_b \cap S} D)$  but not both. Assume that  $y \in \text{vars}(\sum_{D \in V'_b \cap S} D)$ ; the other case is symmetric. Now  $\text{vars}(\sum_{D \in V'_a \cap S} D) \subseteq \{x\}$  and  $\text{vars}(\sum_{D \in V'_b \cap S} D) \subseteq \{x, y\}$ . If  $x \in \text{vars}(\sum_{D \in V'_a \cap S} D)$ , then  $\sum_{D \in V'_a \cap S} D = (x \equiv p_x)$  for a  $p_x \in \{\perp, \top\}$ ,  $\phi_{\text{xor}}^a \wedge \tilde{l}_1 \wedge \dots \wedge \tilde{l}_k \models (x \equiv p_x)$ ,  $\sum_{D \in V'_b \cap S} D = (x \oplus y \equiv p_x \oplus p_y)$ , and  $\phi_{\text{xor}}^b \wedge \tilde{l}_1 \wedge \dots \wedge \tilde{l}_k \wedge (x \equiv p_x) \models y \oplus p_y$ . If  $x \notin \text{vars}(\sum_{D \in V'_a \cap S} D)$ , then  $x \notin \text{vars}(\sum_{D \in V'_b \cap S} D)$ ,  $\sum_{D \in V'_b \cap S} D = (y \equiv p_y)$ , and  $\phi_{\text{xor}}^b \wedge \tilde{l}_1 \wedge \dots \wedge \tilde{l}_k \models (y \equiv p_y)$ . ■